



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/605,173	09/12/2003	ASHOT ANDREASYAN	PR 1803.01 US	2172
31883 7590 09/17/2007 DVA/PIONEER RESEARCH CENTER USA, INC. 2265 E. 220TH STREET LONG BEACH, CA 90810			EXAMINER HA, LEYNNA A	
			ART UNIT 2135	PAPER NUMBER
			MAIL DATE 09/17/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

**Advisory Action
Before the Filing of an Appeal Brief**

Application No.

10/605,173

Applicant(s)

ANDREASYAN, ASHOT

Examiner

LEYNNA T. HA

Art Unit

2135

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 29 August 2007 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☐ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

- a) ☐ The period for reply expires _____ months from the mailing date of the final rejection.
b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
(a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
(b) ☐ They raise the issue of new matter (see NOTE below);
(c) ☒ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
(d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☒ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
The status of the claim(s) is (or will be) as follows:
Claim(s) allowed: _____.
Claim(s) objected to: _____.
Claim(s) rejected: 1-35.
Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

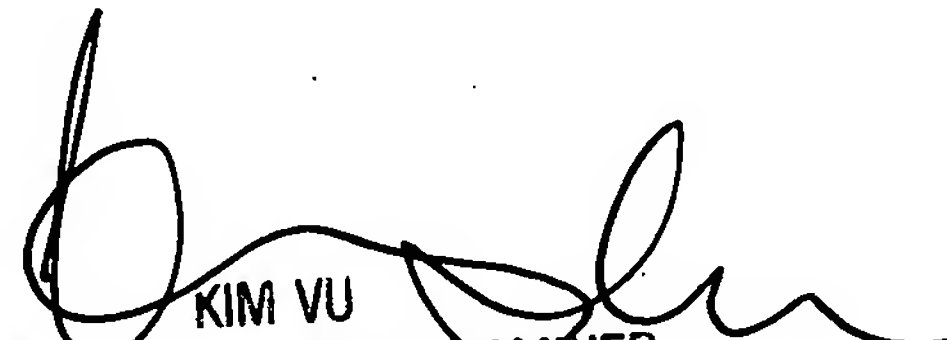
11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because:
See Continuation Sheet.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08) Paper No(s). _____.
13. ☐ Other: _____.

Continuation of 11. does NOT place the application in condition for allowance because: claims 1-35 remains rejected in view of Roy (6,677,888). Amendments made after the Final rejection is not materially reducing or simplifying the issues for appeal will not be entered.

and
according to the argument on pg.10 (last paragraph), applicant argues the invention is not about using a certificate as disclosed in Roy but to utilize parameters from a certificate to generate a secret key by using only 3 exponential operations. First, it is unclear which parameters and which certificate applicant is referring to because the claimed invention recites using a first parameter of a first certificate to generate a first public key and using a second parameter of a second certificate to generate a shared secret key. The claimed invention recites the first parameters being digital signature standard parameters whereas the second parameters does not limit to what can be the parameters for the second certificate. Thus, the parameters from a certificate to generate a secret key corresponds to the claimed second parameters where parameters can broadly be domain parameters, random values, identities, key size, etc. Roy discloses additional data known to both entities such as identities, as well as random values designed that a different shared secret key is computed each time (col.10, lines 13-16). Roy also discusses the domain parameters and key size determine the cryptographic strength (col.10, lines 30-31) and to establish a secret session key, a message is created and signs the message with the signature (col.10, lines 49-52). All these reads on the claimed using parameters to generate a secret key.

According to arguments on pg.11, that unlike Roy, the present invention uses DSA parameters from already issued certificates is traversed because this is not claimed in the independent claims. Ennuendo, a DSA type certificate with DSA parameters are claimed, DSA protocol or process for digital signature algorithm is well known in the art. It is known in the art there involves exponentiations during the process of generating a shared key using DSA type certificates in order to verify its authenticity to each other (peers). Further it is known the exponentiations involves generating a public key for verification which inherently needs a key from each peer whether the keys is asymmetric or symmetric keys is up to the protection. The public/secret key cryptography, a shared secret key generated for a second peer and a shared secret key for the first peer are inherently symmetric keys that is required to verify its authenticity.

According to argument on pg.13, examiner traverses that Yeager does not disclose generating a secret key by 3 exponentiation operations using DSA parameters because Yeager is combined with Roy to teach the obviousness of the Bluetooth technology of the wireless network.


KIM VU
SUPERSENIOR PATENT EXAMINER
TECHNOLOGY CENTER 2100